National Infrastructure Protection Center
CyberNotes

Issue #2000-23 *November 20, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 2, 2000 and November 17, 2000. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Bill Kendrick[1]	GBook.cgi 1.0	Due to the improper validation of user-supplied input to the _MAILTO parameter, a remote malicious user could elevate their privileges or execute arbitrary code.	Upgrade available at: ftp://ftp.sonic.net/pub/users/nbs/unix/www/gbook/gbook.tar.gz	Gbook.cgi Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.

[1] eSecurityOnline.com Free Vulnerability Alert 3145, November 15, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CGI Script Center[2] Windows NT 4.0/2000, Unix	Subscribe Me Lite 2.01	A vulnerability exists that could allow a remote malicious user to delete anyone from the subscription database without needing the administration password.	Unofficial workaround (eSecurityOnline.com): Ensure the addresses.txt file is not stored in a web accessible directory, and control local user access to the server.	Subscribe Me Lite Account Deletion	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Check Point Software[3]	Firewall-1 3.0, 4.0	A vulnerability exists which could let a remote malicious user determine a valid username and attempt a brute force to determine the password. If successful, they could then gain access to the firewall based on that user's privileges.	No workaround or patch available at time of publishing.	Firewall-1 Valid Username Brute Force	Medium/ **High** **(High, if DDoS best – practices not in place.)**	Bug discussed in newsgroups and websites. Exploit has been published.
Compaq[4] Windows NT	Compaq Management Agents for Netware 2.28	A vulnerability exists in the default installation, which could let a malicious user gain access to sensitive system files and gain full administrative control.	Compaq recommends that you disable the web agent until a resolution has been provided.	Compaq Management Agents for Netware Plaintext Password	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Computer Associates[5] Windows NT	InoculateIT 4.53	Multiple vulnerabilities exist which could allow viruses to enter the mail server and arrive to the e-mail recipient without being detected.	No workaround or patch available at time of publishing.	InoculateIT MS Exchange Agent	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
CS&T[6] Unix	Corporate Time for the Web 2.1.2 and previous	A vulnerability exists which could let a malicious user brute force usernames and passwords.	No workaround or patch available at time of publishing.	CorporateTime for the Web Brute Force	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
DC Scripts[7] Windows NT/2000, Unix	DCForum 1.0-6.0	An input validation vulnerability exists in the dcforum cgi script, which could allow a remote malicious user to view arbitrary files on the host and possibly compromise root.	Patch available at: http://www.dcscripts.com/dcforum/dcfNews/124.html	DCForum cgforum.cgi Arbitrary File Disclosure	**High**	Bug discussed in newsgroups and websites.
Flicks Software[8] Windows NT	Authentix 5.1c	A security vulnerability exists which could allow a malicious user to view secured files.	Upgrade available at: http://www.flicks.com/authentix100	Authentix Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[2] eSecurityOnline.com Free Vulnerability Alert 3099, November 2, 2000.
[3] Bugtraq, November 1, 2000.
[4] iXsecurity Security Vulnerability Report, 20001107, November 7, 2000.
[5] Bugtraq, November 10, 2000.
[6] Bugtraq, November 2, 2000.
[7] Cgi Security Advisory #2, November 14, 2000.
[8] Authentix Security Advisory, Authentix100, November 1, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Foundry Networks[9]	BigIron 7.1.09; FastIron 7.1.09; ServerIron 7.1.09	A Denial of Service vulnerability exists in the Telnet login prompt.	No workaround or patch available at time of publishing.	Foundry Networks Telnet Login Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD[10] Unix	FreeBSD 3.0-3.5, 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-STABLE	A vulnerability exists in the TERMCAP environment variable, which could allow a remote malicious user to cause a Denial of Service.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:69/telnetd.patch	FreeBSD Telnetd Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
FreeBSD[11] Unix	FreeBSD 3.5.1, 4.1.1	A buffer overflow vulnerability exists in the html code, which could allow a remote malicious user to execute arbitrary code.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports	FreeBSD Netscape Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
FreeBSD[12] **Unix** ***Updated patch released[13]***	**FreeBSD 3.5x, 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-STABLE, RELEASE**	**A format string vulnerability exists which could let a malicious user corrupt stack variables and execute arbitrary code.**	**Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:62/top.patch** ***Upgrade your vulnerable FreeBSD system to 4.1.1-STABLE or 3.5.1-STABLE.***	**FreeBSD top Format String**	**High**	**Bug discussed in newsgroups and websites.**
FreeBSD[14] Unix	Global port, versions 3.5 through to 3.55	A vulnerability exists in the CGI script generated by the htags utility, which could allow a remote malicious user to execute arbitrary code.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/	FreeBSD Global Htags	**High**	Bug discussed in newsgroups and websites.
GSX[15]	gsx-0.90d gsx-0.90e	A security vulnerability exists which could allow remote malicious users to cause a Denial of Service.	No workaround or patch available at time of publishing	GSX Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard[16] Unix	HP9000 systems running HP-UX 10.10, 10.20, 10.24, 11.00, 11.04	A vulnerability exists in dtterm, which could let a malicious user gain unauthorized privileges.	Apply patches listed below: HP-UX 11.00: PHSS_22320 HP-UX 11.04: PHSS_22548 HP-UX 10.20: PHSS_22319 HP-UX 10.24: PHSS_22546 HP-UX 10.10: not yet available	HP-UX Dtterm Privilege Elevation	Medium	Bug discussed in newsgroups and websites.

[9] Bugtraq, November 11, 2000.
[10] FreeBSD Security Advisory, FreeBSD-SA-00:69, November 15, 2000.
[11] FreeBSD Ports Security Advisory, FreeBSD-SA-00:66, November 6, 2000.
[12] FreeBSD Security Advisory, FreeBSD-SA-00:62, November 1, 2000.
[13] FreeBSD Security Advisory, FreeBSD-SA-00:62, Reissued November 6, 2000.
[14] FreeBSD Ports Security Advisory, FreeBSD-SA-00:64, November 6, 2000.
[15] Securiteam, November 11, 2000.
[16] Hewlett-Packard Security Advisory, HPSBUX0011-128, November 2, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[17] Unix	HP-UX 9.x-11.0	A buffer overflow vulnerability exists that could let a malicious user evaluate privileges and gain root access.	**Recommended Fix:** 1. Find cu % which cu or % find / -name cu –print 2. Disable execute permissions for all users except root or limit usage to a specified group.	HP-UX Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[18] Unix	HP-UX 10.0.1, 10.10, 10.20, 10.24, 11.0, 11.4	A vulnerability exists in the script auto_parms, which could let a malicious user execute arbitrary commands or gain root access.	Apply the appropriate patches. HP-UX 11.00: PHCO_21993 HP-UX 11.04: PHCO_22186 HP-UX 10.20: PHCO_21992 HP-UX 10.24: PHCO_22185 HP-UX 10.10: PHCO_21991 HP-UX 10.01: PHCO_21990	HP-UX auto_parms Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
Hewlett-Packard[19] Unix	HP-UX 10.20	A vulnerability exists which may allow a local malicious user to read any file on the host's filesystem or elevate privileges.	Unofficial workaround (Bugtraq): A workaround is to ensure that /etc/opt/resmon/log is not accessible by anyone other than root.	HP-UX Registrar Local Arbitrary File Read	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[20] Unix	HP-UX 11.0, 11.11	A security vulnerability exists in the default permissions of files and directories, which could allow a malicious user to create a Denial of Service.	Patch available at: HP patch PHSS_22540 ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/ If your installation is running an earlier release of MC/ ServiceGuard, please upgrade to MC/ServiceGuard Version A.11.09 before applying the patch.	HP-UX MC/Service Guard Default Permissions	Low	Bug discussed in newsgroups and websites.
IBM[21] Unix	AIX 3.2.x, 4.1.x, 4.2.x, 4.3.x	A vulnerability exists in the catopen() call which could let a malicious user gain root access.	Workaround available at: ftp://aix.software.ibm.com/aix/efixes/security/locale_format_efix.tar.Z	AIX Locale Subsystem Format String CVE name CAN-2000-0844	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Lawrence Berkeley Laboratory[22] **Unix** ***Corrected patch released[23]***	**tcpdump 3.4, 3.5, 3.5 alpha**	**Several buffer overflow vulnerabilities exist which could let a malicious user gain root access.**	***New patch released:*** ***FreeBSD 3.x:*** ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:61/tcpdump-3.x.patch ***FreeBSD 4.x:*** ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:61/tcpdump-orkaround or **at**	**ch ble at time r Overflow**	**High**	**Bug discussed in newsgroups and websites.**

[17] Bugtraq, November 2, 2000.
[18] Hewlett-Packard Company Security Bulletin, HPSBUX0011-130, November 13, 2000.
[19] Bugtraq, November 8, 2000.
[20] Hewlett-Packard Security Bulletin, HPSBUX0011-129, November 8, 2000.
[21] Securiteam, November 3, 2000.
[22] FreeBSD Security Advisory, FreeBSD-SA-00:61, October 30, 2000.
[23] Updated FreeBSD Security Advisory, FreeBSD-SA-00:61, November 6, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Lotus Development Corporation[24] Windows NT 4.0, Unix	Domino Mail Server 5.0.1-5.0.4, Domino Enterprise Server 5.0.1-5.0.4	A vulnerability exists in the ENVID variable, which could allow a remote malicious user to perform a Denial of Service or execute arbitrary code.	Update Lotus Domino with the following patch: http://www.notes.net/qmrdown.nsf/qmrwelcome?OpenView&Start=1&Count=30&Expand=1	Domino SMTP Server ENVID Buffer Overflow and Denial of Service	**High**	Bug discussed in newsgroups and websites.
Lotus Development Corporation[25]	Lotus Notes Client 5.0-5.0.5	A vulnerability exists in the implementation of the S/MIME standard that could allow a malicious user to corrupt signed messages in transit without notification being sent.	No workaround or patch available at time of publishing.	Lotus Notes S/MIME	Medium	Bug discussed in newsgroups and websites.
Max Feoktistov[26] Windows 95/98	Small HTTP server 2.01	Several Denial of Service vulnerabilities exist when multiple GET, HEAD, or POST commands are requested, when an ServerSidesIncludes (SSI) tag formed a certain way is sent, or when an http request is made without a filename specified.	Upgrade to Small HTTP Server 2.03 available at: http://wwwwin.wplus.net/pp/mrdoors/srv/shttp2.exe	Small HTTP Server Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit has been published.
McAfee[27] Windows 95/98/ME/NT 4.0/2000	VirusScan 4.5	A vulnerability exists in the default installation, which could allow a malicious user to elevate their privileges, add/remove users, modify files, or implant Trojans and viruses.	Install Service Pack 1 for VirusScan. **workaround:** Place quotes around the image path for the McShield AvSyncMgr Service or Change default permissions on "C:\Program Files" and "C:\Program Files\Common Files" so that they may only be written by Local Admin.	VirusScan Unquoted ImagePath	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
McMurtrey/ Whitaker & Associates[28]	Cart32 3.0, 3.1, 3.5	Multiple vulnerabilities exist: a Denial of Service when a specially formed URL is requested, a number of information leakage vulnerabilities, weak encryption of the password, which could reveal server information and possibly allow a full compromise of the server's security.	Part of this issue has been addressed in Cart32 version 3.5a. However, the latest build has not addressed the 'CheckError?error=53' portion. http://www.cart32.com/latestbuilds.asp	Cart32 Multiple Vulnerabilities	Low/**High**	Bug discussed in newsgroups and websites. Exploits have been published.

[24] S.A.F.E.R. Security Bulletin, 001103.EXP.1.9, November 3, 2000.
[25] Securiteam, November 10, 2000.
[26] Securiteam, November 15, 2000.
[27] NTBugtraq, November 3, 2000.
[28] Xato Network Security Advisory, XATO-112000-01, November 9, 2000.

		rk	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-088.asp	Microsoft 2000 Exchange User Account	Medium	Bug discussed in newsgroups and websites.
Microsoft[30] Windows NT 2000	Indexing Services for Windows 2000	A vulnerability exists in the indexing service, which could let a remote malicious user gain sensitive information.	Unofficial workaround (Georgi Guninski): Disable Active Scripting or Indexing service.	Indexing Services for Windows 2000 File Verification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[31] Windows NT 4.0	Internet Information Server 4.0	A buffer overflow vulnerability exists in the ASP ISAPI file parsing mechanism, which could let a malicious user gain SYSTEM level access or run arbitrary code.	This issue has been resolved by a number of Microsoft IIS patches, including the following: http://download.microsoft.com/download/winntsp/Patch/Q274149/NT4/EN-US/secsesi.exe	IIS ISAPI Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[32] Windows NT 4.0/2000	Internet Information Services 4.0, 5.0	A vulnerability exists when IIS receives a specially formed request for an executable file followed by operating system commands, which could let a malicious user read system files and run arbitrary system commands.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-086.asp	IIS Web Server File Request Parsing CVE name CAN-2000-0886	**High**	Bug discussed in newsgroups and websites.
Microsoft[33] Windows NT	Windows NT Terminal Server	A buffer overflow vulnerability exists which could allow a malicious user to cause the Terminal Server to fail or to execute hostile code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-087.asp	Windows NT Terminal Server Login Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[29] Microsoft Security Bulletin, MS00-088, November 16, 2000.
[30] Georgi Guninski Security Advisory #27, November 10, 2000.
[31] Bugtraq, November 3, 2000.
[32] Microsoft Security Bulletin, MS00-086, updated November 10, 2000.
[33] Microsoft Security Bulletin, MS00-087, November 8, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[34] BeOS	BeOS r4.5, r4.5-2, r5 pro; Felix-2-3-R4 (IRC Client); Baxter (IRC Client); Bowser (IRC Client); PostMaster-1.0 (E-mail Client); RobinHood-1.1 (HTTPD)	Several programs that were built for BeOS (and are bundled with it) suffer from buffer overflow problems. These buffer overflows can be used to execute arbitrary code.	Contact your vendor to see if a patch is available. **PostMaster:** Upgrade to PostMaster version 1.1.1 available at: http://kennyc.com/postmaster/download.html	Multiple Vendor BeOS Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[35] Unix	Caldera OpenLinux 2.4; Debian Linux 2.2, 2.3; RedHat Linux 6.2 & 6.2E alpha, i386, sparc, 7.0; SGI IRIX 5.2, 5.3, 6.3; Sun Solaris 2.6_x86HW3/98, 2.6_x86, 2.6, 2.5.1_x86, 2.5.1_ppc, 2.5.1, 2.5_x86, 2.5, 2.4_x86	A vulnerability exists an e-mail message with a carefully formed string in the 'Reply-To' field includes meta-characters, which could let a malicious user elevate his privileges and possibly gain root access.	No workaround or patch available at time of publishing.	Multiple Vendor Mail 'Reply-To' Field	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[36]	id Software Quake 1.9; J. P. Grossman ProQuake 1.0	A vulnerability exists in the way UDP packets are handled, which could let a remote malicious user crash the server.	No workaround or patch available at time of publishing.	Quake Server Empty UDP Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[37] Windows, Unix	ISC BIND 8.2-8.2.2-P6	Two Denial of Service vulnerabilities exist: one in the Compressed Zone Transfer (ZXFR) functionality of BIND; and the second in the 'srv' record.	Upgrade to BIND 8.2.2-P7 at: ftp://ftp.isc.org/isc/bind/src/8.2.2-P7/bind-src.tar.gz	Multiple Vendor BIND Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[34] Bugtraq, November 14, 2000.
[35] Bugtraq, November 5, 2000.
[36] Bugtraq, November 2, 2000.
[37] CERT Advisory, CA-2000-20, November 14, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[38] Unix	Sun StarOffice 5.2	A symbolic link vulnerability exists which can allow malicious users to read and write to restricted files, or plant Trojans.	Unofficial workaround (Securiteam): A workaround is to create a symbolic link from /tmp/soffice.tmp to a directory inside the your home directory which is inaccessible to anyone but yourself.	StarOffice /tmp Directory Symbolic Link	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[39] Unix	SuSE. Linux 6.4,7.0; RedHat Linux 7.0; Immunix OS 6.2, 7.0-beta; Linux-Mandrake 7.1, 7.2 (GNU Linux modutils 2.3.9)	A vulnerability exists in the modprobe tool, which could let a malicious user gain root access.	**SuSE:** ftp://ftp.suse.com/pub/suse **RedHat:** ftp://updates.redhat.com/ **Immunix:** http://www.immunix.org:8080/ImmunixOS/6.2/updates **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3.	Linux Modprobe Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[40, 41] **Unix** ***RedHat also vulnerable[42]***	**GNOME GnoRPM 0.94 and earlier; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1;** ***RedHat Linux 6.1, 6.2, and 7.0***	**A vulnerability exists in the way tmp files are handled which could allow a local malicious user to cause an arbitrary file to be overwritten by the root user.**	**A new release of GnoRPM (0.95.1) is available at: ftp.gnome.org/pub/GNOME/stable/sources/gnorpm/gnorpm-0.95.1.tar.gz** **Conectiva: ftp://atualizacoes.conectiva.com.br/** **MandrakeSoft: http://www.linux-mandrake.com/cooker/** ***RedHat:*** **ftp://updates.redhat.com/**	**GnoRPM Arbitrary File Overwrite**	High	**Bug discussed in newsgroups and websites.**
Network Associates[43] Windows NT	Sniffer Agent 3.0.10	Several buffer overflow and protocol vulnerabilities exist which could allow a remote malicious user to cause a Denial of Service or the ability to recover login passwords, take control of the agent, delete logs, execute arbitrary code, and gain System-level privileges.	An upgrade is recommended.	Sniffer Agent Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.

[38] Securiteam, November 9, 2000.
[39] Bugtraq, November 12, 2000.
[40] eSecurityOnline.com, October 4, 2000.
[41] Conectiva Linux Security Announcement, October 3, 2000.
[42] Red Hat, Inc. Security Advisory, RHSA-2000:072-07, November 2, 2000.
[43] Securiteam, November 6, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Oliver Fourdan[44] Unix	Xfce 3.5, 3.5.1	A vulnerability exists in the startup script, which could let a malicious user monitor and control the contents of the display window and monitor input from keyboard and mouse devices.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-5-current/x11-wm	Xfce Port Display	Medium	Bug discussed in newsgroups and websites.
OpenBSD[45, 46] Unix	OpenSSH 2.2.x	A vulnerability exists in the OpenSSH client, which could allow a malicious user unauthorized access to restricted resources.	Upgrade available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-2.2.0.tgz	OpenSSH Client Unauthorized Remote Forwarding	Medium	Bug discussed in newsgroups and websites.
PeleSoft[47] Windows 95/98/NT 4.0/2000	NetSnap 1.2	A vulnerability exists in the way GET requests are handled which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.netsnap.com/	NetSnap Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Poll It[48]	Poll It v2.0	A vulnerability exists in the CGI script, which could enable a remote malicious user to execute arbitrary commands.	Patch available at: http://www.cgi-world.com/pollit.html	Poll It CGI Arbitrary Command	**High**	Bug discussed in newsgroups and websites. Exploit script has been published
Recourse Technologies[49]	ManTrap 1.6.1	Numerous vulnerabilities exist due to a failure to handle exceptional conditions, which could be used to cause a Denial of Service, or read/modify data on the system.	Upgrade to ManTrap v2.0 with the most recent patch set. Please contact Recourse Technologies for information on how to obtain v2.0 and/or the current patch set at: http://www.recourse.com As of this date, Recourse had not been able to repair the 'crash' utility problem, so it still exists in the newest release.	ManTrap Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[50] **Unix** ***Multiple Vendor vulnerability[51]***	**Dump 0.4b15-1** Trustix Secure Linux 1.1	**A vulnerability exists in the dump package that allows suid root execution of other executables. Successful exploitation of this vulnerability results in root compromise.**	***Trustix patch available at:*** http://www.trustix.net/download/Trustix/updates/1.1/RPMS/	***Multiple Vendor dump Insecure Environment Variables***	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[44] FreeBSD Ports Security Advisory, FreeBSD-SA-00:65, November 6, 2000.
[45] Linux-Mandrake Security Update Advisory, MDKSA-2000:068-1, November 15, 2000.
[46] Trustix Security Advisory, November 15, 2000.
[47] Strumpf Noir Society Advisories, November 16, 2000.
[48] Securiteam, November 6, 2000.
[49] Fate Research Labs Advisory, November 1, 2000.
[50] Red Hat, Inc. Security Advisory, RHSA-2000:100-02, November 2, 2000.
[51] Trustix Security Advisory, November 3, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
RedHat[52] **Unix** ***RedHat issues updated patches[53]***	**Linux 6.0, 6.1, 6.2.**	**The usermode package allows unprivileged users logged in at the system console to run the halt, poweroff, reboot, and shutdown commands without using the superuser's password.** ***Updated usermode packages are now available for Red Hat Linux 6.x and 7.***	**Update available at: ftp://updates.redhat.com**	**RedHat Usermode Denial of Service**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
RedHat[54] Unix	RedHat Linux 5.2, 6.0, 6.1, 6.2, i386, alpha, sparc, 6.2EE - i386, 7.0 i386	A vulnerability exists when specfic headers are added to messages, which could let a malicious user manipulate mail folders containing those messages.	Update available at: ftp://updates.redhat.com/	RedHat Pine Denial of Service	Medium	Bug discussed in newsgroups and websites.
RedHat[55] Unix	RedHat restore 0.4b15	A vulnerability exists in the RSH (remote executed shell) parameter that could allow a malicious user to elevate their permissions. Exploitation of this vulnerability can result in root compromise.	No workaround or patch available at time of publishing.	RedHat Restore Insecure Environment Variables	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Rob Flynn[56] Unix	Gaim 0.10.3, 0.10x	A buffer overflow vulnerability exists which could allow a remote malicious user to execute shell code with the same permissions as the Gaim user. If properly exploited, this can yield root privileges.	Patch available at: ftp://ftp.marko.net/pub/gaim/gaim-0.10.2-0.10.3.patch.gz	Gaim Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Samba[57] Unix	Samba 2.0.7	A vulnerability exists in the utility titled SWAT (Samba Web Administration Tool), which could allow a malicious users to gain root access.	No workaround or patch available at time of publishing.	Samba SWAT Logfile Permissions	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[52] Red Hat, Inc. Security Advisory, RHSA-2000:053-04, August 29, 2000.
[53] Red Hat, Inc. Security Advisory, RHSA-2000:075-07, November 8, 2000.
[54] Red Hat, Inc. Security Advisory, RHSA-2000:102-04, November 10, 2000.
[55] Bugtraq, November 4, 2000.
[56] Bugtraq, November 13, 2000.
[57] Bugtraq, November 10, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Symantec[58] Windows NT 4.0	I-Gear 3.5.6	A vulnerability exists in the Microsoft Proxy, which could let a malicious user submit long URLs, resulting in the inability to view the logfile.	No workaround or patch available at time of publishing.	I-Gear for Microsoft Proxy long URL	Low	Bug discussed in newsgroups and websites.
TServ Incorporated[59] Windows 95/98/NT 4.0/2000	RideWayPN 6.22	A vulnerability exists when the proxy server is running with the Telnet proxy enabled, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	RideWayPN Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published
Volano LLC[60] Unix	VolanoChat Pro 2.1	A vulnerability exists in the configuration file "properties.txt," which could let a malicious user obtain passwords and create arbitrary files.	Recommended Fix: As a workaround solution, remove the world readable permissions on the configuration file with the following: *chmod -s* *permissions.txt* Do not run the server as a privileged user and block access to the administrative port from unauthorized sources.	VolanoChatPro Local Password Disclosure	**High**	Bug discussed in newsgroups and websites.
Voyant Technologies[61] OS/2, Unix	Sonata v3.x on Solaris 2.x.; Sonata bridge OS/2 Warp	Six vulnerabilities exist: reused default user accounts and passwords, easily guessable passwords, poor file permissions, lack of host hardening, X console authentication has been disabled, and hard coded default passwords which could led to a root compromise.	Please contact Voyant technologies for assistance at: Http://www.voyanttech.com/displaypage.cfm?pid=27&toppid=22	Sonata Conferencing Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
YaBB[62]	YaBB 9.11.2000	An input validation vulnerability exists in the 'catsearch' field which could let a remote malicious user execute an arbitrary command through a specially crafted URL.	No workaround or patch available at time of publishing.	YaBB Search.pl Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[58] Securiteam, November 3, 2000.
[59] eSecurityOnline.com Free Vulnerability Alert 3149, November 15, 2000.
[60] eSecurityOnline.com Free Vulnerability Alert 3124, November 8, 2000.
[61] Vapid Labs Advisory, 10132000-01, November 7, 2000.
[62] Securiteam, November 8, 2000.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 2, 2000 and November 17, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 33 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 17, 2000	Its4-1.1.1.tgz	ITS4 scans C and C++ source code, looking for function calls that have potential security vulnerabilities.
November 17, 2000	Vixie-cron.sh	Script which exploits the Vixie crontab local root insecure fopen() call vulnerability.
November 16, 2000	1080r.c	Script which exploits the Socks5 v1.0r10 remote buffer overflow vulnerability.
November 15, 2000	Bsdi_elm.c	Script which exploits the BSDI Elm 2.4 local buffer overflow vulnerability.
November 15, 2000	Deb_gnomehack.c	Script which exploits the Gnomehack v1.0.5 local buffer overflow vulnerability.
November 15, 2000	Phx.c	Script which exploits the Phf remote buffer overflow vulnerability for Linux x86.
November 14, 2000	Bsdi_filter.c	BSDI /usr/contrib/bin/filter v2.x local buffer overflow exploit.
November 14, 2000	Local_nonexec_sun.c	Script which exploits the Solaris Sparc 2.6/7 local root libc locale vulnerability.
November 14, 2000	Traceroot2.c	Script which exploits the local root LBNL traceroute v1.4a5 vulnerability.
November 13, 2000	Cons.saver.txt	Proof of concept exploit for the Midnight Commander package Denial of Service vulnerability.
November 13, 2000	Exchange.dos.txt	Remote Denial of Service exploit for Microsoft Exchange 5.5 SP3 Internet Mail Service vulnerability.
November 13, 2000	**Guninski27.txt**	**Demonstration exploit code for the IE 5.x, Outlook, and Outlook Express vulnerability, which allows searching for files with specific name or content.**
November 13, 2000	Ncpquery-1.2.tgz	Tool that allows probing of a Novell Netware 5.0/5.1 server running IP that discloses account names, server services, and other various objects.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 13, 2000	Ssldump-0.9b1.Tar.gz	An SSLv3/TLS network protocol analyzer that identifies TCP connections on the chosen network interface and attempts to interpret them as SSLv3/TLS traffic.
November 12, 2000	Rh7-modprobe.sh	Script which exploits the Linux Modprobe Arbitrary Command Execution vulnerability.
November 11, 2000	Inetdfun.tar.gz	A public version of an inetd backdoor which uses ICMP to trigger a remote shell.
November 10, 2000	**Gimme-login.sh**	**Script which exploits the SAMBA SWAT Logfile Permissions vulnerability.**
November 10, 2000	Sdebug.tgz	An ELF binary segment scanner with a console ncurses interface.
November 8, 2000	Nessus-1.0.6.tar.gz	A full featured remote security scanner for Linux, BSD, Solaris, and some other systems that is multithreaded, plugin-based, and performs over 530 remote security checks.
November 8, 2000	Saint-3.1.1.beta1.tar.gz	An updated version of SATAN.
November 7, 2000	Krnl-dos.c,	Proof of concept exploit for the OpenBSD and NetBSD Denial of Service UVM vulnerability.
November 7, 2000	Rcf-5.0.1.tar.gz	An Ipchains-based firewall setup script with easy support for many network services, masquerading, port forwarding, and IP accounting.
November 6, 2000	Quakeworldex.txt	Proof of concept exploit for the Quake World v2.30 rcon buffer overflow vulnerability.
November 5, 2000	**Exgsx.c**	**Exploit script for the remote Denial of Service Gsx-0.90e vulnerability.**
November 5, 2000	Pollex.pl	Perl script that exploits the remote Poll It CGI v2.0 vulnerability.
November 4, 2000	Ads_cat.zip	A utility for writing to NTFS's Alternate File Streams, providing a way to hide data on a Windows NT system in a manner which makes it completely invisible to all users, administrators, and disk size commands.
November 4, 2000	Eeye.iishack-1.5.txt	Exploit for the IIS 4.0 and 5.0 .asp file parsing buffer overflow vulnerability.
November 4, 2000	Natas.zip	An advanced network packet capturing and analysis program designed for Windows 2000, which works with the new Winsock v2.2 and features the ability to filter traffic by address and port, log packets, parse out passwords, and requires no driver.
November 4, 2000	**Restore-cool.sh**	**Script which exploits the Linux Restore Insecure Environment Variables vulnerability.**
November 4, 2000	Ruleset-retrieve.c	Script which obtains the newest Snort IDS ruleset from www.snort.org or whitehats.com and inserts your IP address into the appropriate areas.
November 4, 2000	Winzapper.zip	A tool that allows you to erase event records selectively from the Security Log in Windows NT 4.0 and Windows 2000.
November 3, 2000	Mantrap.c	Script which exploits the ManTrap Multiple vulnerabilities.
November 3, 2000	Xrestore.c	Restore (/sbin/restore) v0.4b15 local root exploit.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

The CERT Coordination Center has recently issued an alert regarding of two serious Denial-of-Service vulnerabilities in the Internet Software Consortium's (ISC) BIND software. For more information, please see CERT Advisory CA-2000-20, located at: http://www.cert.org/advisories/CA-2000-20.html**.**

A new variant of the SubSeven Trojan Horse has been discovered in the wild. For more information please see NIPC ADVISORY 00-056 located at:
http://www.nipc.gov/warnings/advisories/2000/00-056.htm

Numerous sites that still run an old version of Apache have been victimized by a Windows-based DDoS attack originating from over 500 different IP addresses.

A steady number of reports have been received of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

Intruders are using scripts and toolkits to automate attacks against the input validation problem in rpc.statd and the input validation problems in FTPD, the site exec vulnerability. For more information, see the CERT advisory located at: http://www.cert.org/incident_notes/IN-2000-10.html.

Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.

Other:

An update has been issued to NIPC Assessment 00-057, advising recipients of the ongoing cyber denial-of-service (DoS) attacks against Palestinian- and Israeli-related web sites. For more information, please see NIPC Advisory 00-058 located at:
http://www.nipc.gov/warnings/advisories/2000/00-058.htm.

Several instances of remote self-updating viruses have been reported. In addition, the most recent virus incorporates strong cryptography to avoid detection.

NIPC has issued an assessment on the W32 Navidad@M Worm. For more information, please see NIPC Assessment 00-059 located at: http://www.nipc.gov/warnings/assessments/2000/00-059.htm.

There has been a compromise of two SUN security certificates on any system whose web browser has accepted SUN certificates with the following numbers: 3181 B12D C422 5DAC A340 CF86 2710 ABE6 (Internet Explorer), and 17:05:FB:13:A2:2F:9A:F3:C1:30:F5:62:6E:12:50:4C (Netscape). For more information, see CERT Advisory, CA-2000-19 Revocation of Sun Microsystems Browser Certificates, located at: http://www.cert.org/advisories/CA-2000-19.html.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. WARNING: at times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **213** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **598** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	VBS/LoveLetter	Script	Stable	March 2000
2	PE_MTX.A	File Infector, Trojan	Slight increase	September 2000
3	VBS/Kakworm	Script	Slight decrease	December 1999
4	W32/SKA	File	Increase	March 1999
5	VBS/Stages	Script	Slight decrease	June 2000
6	W97M/Marker	Macro	Increase	August 1998
7	W97M/Ethan.A	Macro	Decrease	February 1999
8	FunLove	File	Slight increase	November 1999
9	W32/PrettyPark	File	Return to table	June 1999
10	W95/CIH	File	Return to table	April 1999

PE_HIV (Aliases: W32.HIV, HIV) (File Infector Virus): This PE virus infects all Win 32 Applications with file sizes ranging from 16,384 bytes up to 4,294,967,295 bytes or 4,294 Gigabytes. It infects these files by appending its code to the files. Upon execution, this virus modifies system components and disables file protection. It also automatically downloads a file from the virus writer's website. This file may be an upgraded version of the virus or any other malicious code, depending on the virus writer. The virus also overwrites target HTML files. Once its anti-debugging routines are executed, the virus hangs the infected PC using the System Bootstrap Loader.

VBS_FABLE (Aliases: I-Worm.PIF.Fable, FABLE) (Visual Basic Script Worm): This Visual Basic Script virus uses MS Outlook to propagate. It sends itself as an attachment, FABLE.PIF, to all lists in the address book of the infected user.

VBS/LoveLet-BT (Visual Basic Script Worm): This is a variant of the VBS/LoveLet-AS Word macro virus, which is a corrupted version of VBS/LoveLet-AS. Although the corruption to the virus code is significant, the virus still manages to replicate.

VBS_LUCKY2 (Alias: VBS.LUCKY2) (Visual Basic Script Worm): This is a destructive Visual Basic Script that overwrites vbs files in the current directory with its code if the system supports Windows Scripting Host. It randomly displays a message box and adds an entry in the Favorites folder.

VBS_TERRA.A (Alias: TERRA.A) (Visual Basic Script Worm): This is a VBScript worm that searches the user system for passwords and then sends them by e-mail to a certain address.

W32/Hybris-B (Windows 32 Executable File Virus): This is an e-mail-aware worm that modifies WSOCK32.DLL. It attempts to e-mail a copy of itself as an attachment along with all outgoing e-mails from an infected computer. The worm then scans sent and received data for any e-mail addresses, and sends copies of itself to these addresses. The subject, text, and name of the attached file are chosen randomly by the worm. Hybris also contains several (up to 32) components (plug-ins) in its program code, and executes them depending on its needs. The worm functionality is mostly defined by the plug-ins, which are stored in the body of the worm and are encrypted by a very strong cryptographic algorithm. The virus maintains the functionality of its plug-ins via the "alt.comp.virus" conference on the Usenet, and downloads any upgraded or missing plug-ins from the conference or the author's Web site, if available.

W32/Hybris-C (Win32 Worm): This virus has been reported in the wild. It is a worm capable of updating its functionality over the Internet, which consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects wsock32.dll. Whenever an e-mail is sent, the worm attempts to send a copy of itself in a separate message to the same recipient. The text of the e-mail message is determined by one of the installed components, and can be changed by the upgrading mechanism detailed below. The worm checks the language settings of the computer it has infected, and selects a message accordingly from: English, French, Portuguese, or Spanish. The methods for upgrading the worm can also be changed as they are also upgradable components. One of the upgrading techniques attempts to download the encrypted components from a website, which is presumably operated by the worm author. This website has since been disabled. However, this component could be upgraded to have a different web address. The other method involves posting its current plug-ins to the Usenet newsgroup alt.comp.virus, and upgrading them from other posts by other infections of the worm. These are in the encrypted form, and have a header with a four character identifier and a four character version number, in order for the worm to know which plug-ins to install. Another component of the worm searches the PC for .ZIP and .RAR archive files. When it finds one, it searches inside for a .EXE file, which it renames to .EX$, and then adds a copy of itself to the archive using the original filename.

There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour at any day in the year 2001, displays a large animated spiral in the middle of the screen, which is difficult to close. There is also a component that applies a simple polymorphic encryption to the worm before it gets sent by e-mail. By upgrading this component the author is able to completely change the appearance of the worm in unpredictable ways in an attempt to defeat anti-virus products detecting it.

W32/Music (Alias: W32/Music@m) (Win32 Worm): This is an e-mail-aware Win32 worm. When an infected file is executed, the worm waits a few minutes before attempting to connect to several Internet websites. It attempts to download an updated version of itself from these websites. The worm then tries to send itself to e-mail addresses found on the infected PC. The e-mail message it sends varies depending on the version of itself that has downloaded from the web, but the message text probably would similar to:

"Hi, just testing e-mail using Merry Christmas music file, you'll like it."

The worm is attached as a file called music.com, music.exe or music.zip. When this file is run, the worm attempts to play the first few bars of the song "We wish you a Merry Christmas" and displays a cartoon of Santa Claus with the caption "Music is playing, turn on your speaker if you have one" or "There is error in your sound system, music can't be heard." When it has finished playing the music, it will then display "Merry Christmas" and start playing the music again.

W32/Verona (Win32 Worm): This virus has been reported in the wild. It is an e-mail-aware worm that arrives in an infected e-mail, with two attached files: MYJULIET.CHM and MYROMEO.EXE.

When the e-mail is viewed using Microsoft Outlook, the attachments are automatically saved to C:\windows\temp and a script embedded in the e-mail body is run to view MYJULIET.CHM using the Windows Help browser. This causes MYROMEO.EXE to be executed. The MYROMEO.EXE program attempts to use a list of six SMTP servers to forward itself to addresses in your Microsoft Outlook address book.

W97M/Bridge (Word 97 Macro Virus): This virus uses the same stealth techniques as most macro viruses which affect Microsoft Word. It disables the macro antivirus protection, so that users cannot enable or disable the macros in Word documents opened.

W97M_YOUS.A (Alias: YOUS.A) (Word 97 Macro Virus): This is a macro virus that infects Word documents and modifies the global template. It carries a payload that modifies the network password of the infected system if the current day is from 12 to 22.

WM97/Killdll-B (Word 97 Macro Virus): The virus attempts to delete the first DLL it finds in the \Windows\System subdirectory.

WM97/Marker-BR (Alias: W97M.Marker.BO) (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus. The virus drops the file PHIE.HTML in the Windows directory and attempts to set that file as the wallpaper, which is a poem on a yellow background with the title "a Poet For My Dear Love."

WM97/Marker-FR (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus, created by an interaction between a member of the WM97/Marker family and a user macro.

WM97/Metys-F (Word 97 Macro Virus): This virus has been reported in the wild. It is a minor variant of the WM97/Metys-D Word macro virus, which spreads but does not have a working payload.

WM97/Myna-Z (Word 97 Macro Virus): This is a variant of WM97/Myna-C. The virus displays error messages when it replicates.

WM97/Story-Y (Word 97 Macro Virus): The virus has been created by merging the WM97/Story-A and WM97/Pri Word macro viruses.

WM97/Thus.BH (Aliases: W97M.CELEBRATE.A, W97M/Thus.gen) (Word 97 Macro Virus): This macro virus infects both Word documents and templates. It disables Word's macro virus protection and denies access to macro codes unless Alt-F11 is pressed. On the 11th of each month, this virus modifies the AUTOEXEC.BAT file to display various messages upon system bootup. It also deletes C:\WINDOWS\COMMAND\QBASIC.EXE.

WM97/Thus-BU (Word 97 Macro Virus): This is a variant of the WM97/Thus-A Word macro virus.

WM97/Vesn-A (Word 97 Macro Virus): The virus changes the directory in which User Templates and NORMAL.DOT are stored to "oldpath\normal." For instance, if the directory used to be: C:\Program Files\Microsoft Office\Templates, the virus will change it to: C:\Program Files\Microsoft Office\Templates\normal.

WM97/Wrench-F (Word 97 Macro Virus): When you try to access the Visual Basic Editor, the virus displays the Office Assistant with a message entitled "Skyline MV." The text of the message reads: "You thought you got rid of me, but I'm Still here, better and stronger!."

XM97/Slacker-B (Excel 97 Macro Virus): The virus contains code that attempts to delete files on the C: drive.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last six months and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
Backdoor/Doly.17		CyberNotes-2000-16
BackDoor-GZ		CyberNotes-2000-18
BackDoor-HC		CyberNotes-2000-18
Backdoor-HD		CyberNotes-2000-18
BCK/Sub7.Apocalypse		**Current Issue**
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		CyberNotes-2000-15
Drat	v1.0 - 3.0b	CyberNotes-2000-09
Erap Estrada		CyberNotes-2000-18
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hooker-E		CyberNotes-2000-19
ICQ PWS		CyberNotes-2000-11
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
JS_SEEKER.B		CyberNotes-2000-22
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Mosaic	v2.00	CyberNotes-2000-16
Multijoke.B		CyberNotes-2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09, CyberNotes 2000-12

Trojan	Version	Issue discussed
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		CyberNotes-2000-18
PALM_VAPOR.A		CyberNotes-2000-19
PE_MTX.A		CyberNotes-2000-18
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09, CyberNotes 2000-12
Qaz.A	W32.HLLW.Qaz.A	CyberNotes-2000-20, CyberNotes-2000-16
QDel121		**Current Issue**
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
SubSeven	DEFCON8 2.1 Backdoor	CyberNotes-2000-21
Troj/Simpsons		CyberNotes-2000-13
TROJ_BATMAN		CyberNotes-2000-20
TROJ_BLOODLUST		CyberNotes-2000-21
TROJ_BUTANO.KILL		CyberNotes-2000-19
Troj_Dilber		CyberNotes-2000-14
TROJ_FELIZ		CyberNotes-2000-22
TROJ_IGMNUKE		CyberNotes-2000-20
TROJ_KILLME		CyberNotes-2000-20
TROJ_MSINIT.A		CyberNotes-2000-21
TROJ_MYPICS.F		**Current Issue**
TROJ_NAVIDAD.A		**Current Issue**
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_ROCKET		CyberNotes-2000-22
TROJ_SCOOTER		CyberNotes-2000-19
TROJ_SONIC		CyberNotes-2000-22
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_SUB7.214DC8		CyberNotes-2000-21
TROJ_SUB7.382883		CyberNotes-2000-21
TROJ_VBSWG		CyberNotes-2000-16
Trojan/Anything		**Current Issue**
Trojan/ICQ		CyberNotes-2000-20
Trojan/Parkinson		CyberNotes-2000-21
Trojan/PSW.StealthD		CyberNotes-2000-19
Trojan/Varo31		CyberNotes-2000-19
Trojan/Win32		CyberNotes-2000-21
VBS_MAILPEEP		CyberNotes-2000-22

Trojan	Version	Issue discussed
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

BCK/Sub7.Apocalypse: This is a Backdoor Trojan which is made up of three files: the Server program (that is automatically installed in the victim computer); the Client program (located in the hacker's computer and handled by them), and a configuration program (which indicates the Trojan how to operate). Through the server program, the Trojan deals with the services requested by the client program. In order to carry out its actions, BCK/Sub7.Apocalypse changes a certain entry in the Windows Registry, opening the TCP 123 communication port through which it communicates. The client can then perform the following actions on the infected computer: it opens the CD-ROM tray, it automatically moves the mouse pointer, and it causes the task bar or start button to disappear, etc. Together with these not-so-destructive actions, BCK/Sub7.Apocalyse can perform other dangerous actions revealing confidential information in the victim computer.

QDel121: When ran, this Trojan deletes the current wallpaper .BMP file. It then creates the following registry key value to instruct Windows to launch the program at Startup: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WK=WK.EXE

Trojan/Anything: This Trojan is aimed at reaching other computers systems through a file with an icon common to executable MS/DOS files. When the file is run, this malicious code copies itself (ANYTHING.EXE) to the C:\WINDOWS directory. It also changes the system in order to ensure its presence every time the system is started up.

TROJ_EVIL (Aliases: FaceOfEvil, QZap160, EVIL): This DOS Trojan blacks out the screen and overwrites the diskette in drive A:\ making it unreadable and inaccessible. This message is then displayed:

> "Face Of Evil v.1.02
> Copiando los archivos necesarios en disko.:!"
> [translated: Copying the necessary archives to disk]

If a diskette is not present at the time of execution this message will still be displayed; however, no damage will occur.

TROJ_MYPICS.F (Aliases: MYPICS.F, W32/Mypics.36352.b@MM, I-Worm.MyPics.f, W32.Mypicks.C.Worm): This destructive Trojan propagates via e-mail. Once it is executed, it modifies the AUTOEXEC.BAT file to format the infected user's hard drive. When the system is rebooted after infection, drive C:\ is formatted under a new volume label, which is erased after formatting is completed.

TROJ_NAVIDAD.A (a.k.a. Win32.Watchit): This is a new e-mail worm, which has been reported in-the-wild. The worm arrives in an e-mail message with an attachment called NAVIDAD.EXE. If the attached program is launched, it displays a dialog box containing the text "UI." It then attempts to read new e-mail messages and to send itself to the senders' addresses. The worm copies itself into the Windows and Windows system directories with the filenames WINSVRC.VXD and WINSVRC.EXE and changes the registry so that it runs on Windows startup and before any file is run. The worm also installs itself into the system tray. If the user clicks on the icon, it displays a dialog box with the text "Nunca presionar este boton." If the user clicks the button, the worm displays a dialog box with the title "Feliz Navidad" and the text "Lamentablemente cayo en la tentacion y perdio su computadora." TROJ_NAVIDAD.A also contains a mass-mailing payload, which sends an infected copy of the Trojan to all lists in the Microsoft Outlook address book of the infected user.